

CHECKLISTE

Standards für agentisches Engineering

Das Disziplinblatt für Teams, die KI-Agenten Code schreiben lassen
- dieselben Regeln, die wir täglich auf unsere eigenen Repositories
anwenden.

Warum Disziplin, nicht Werkzeuge, der schwierige Teil ist

Ein Agent, der Code schreibt, ist ein schneller Junior mit unendlicher Ausdauer und ohne Erinnerung an Konsequenzen. Er liefert um 3 Uhr nachts plausible Diffs und - unbeaufsichtigt - plausiblen Schaden. Die Lösung ist kein besseres Modell, sondern dieselbe Engineering-Disziplin, die gute Teams bereits haben - durchgesetzt dort, wo der Agent sie nicht umgehen kann: in Branches, Reviews, CI und Merge-Regeln.

Die Checkliste, nach der wir arbeiten

- ☐ Agenten arbeiten nur auf Feature-Banches - direkte Commits auf main sind per Branch-Protection verhindert, nicht per Konvention
- ☐ Jede Agenten-Änderung kommt als Merge Request mit einer Beschreibung, die ein Mensch geschrieben oder geprüft hat - das 'Warum' wird nie still generiert
- ☐ CI muss vor dem Merge grün sein und der Merge-Button braucht einen Menschen - eine grüne Pipeline ist ein Beleg, keine Erlaubnis
- ☐ Diffs werden wie bei jedem Contributor geprüft: Secrets, Lizenzheader, neue Abhängigkeiten und generierte Dateien bekommen explizite Aufmerksamkeit
- ☐ Secrets gelangen nie in den Agentenkontext - Zugangsdaten leben im Secret Store; erreicht ein Wert ein Transkript, wird er als Incident rotiert
- ☐ Agenten verifizieren am echten System, nicht an Annahmen - eine Behauptung wie 'deployed' oder 'merged' wird durch Lesen des tatsächlichen Zustands bestätigt
- ☐ Lockfile- und Dependency-Updates gehören dem Dependency-Bot (Renovate) - Agenten konkurrieren nicht auf demselben Branch damit
- ☐ Destruktive Operationen brauchen eine explizite menschliche Anweisung - Force-Push, Deletes und History-Umschreibungen sind nie aus dem Kontext ableitbar
- ☐ Generierte Artefakte sind reproduzierbar - ein Skript im Repository baut sie neu, sodass der Diff geprüft statt geglaubt werden kann
- ☐ Der Zustand nach dem Merge wird verifiziert - die angewandte Revision im Deployment entspricht dem gemergten Commit, nicht nur einer grünen Pipeline

Jede dieser Regeln wird durch Infrastruktur durchgesetzt - Branch Protection, Pflicht-Pipelines, Secret Stores - nicht darauf vertrauend, dass der Agent sie sich merkt.

Was das bringt

Tempo ohne Audit-Schulden. Unsere Agenten liefern unter diesen Regeln mehrere Merge Requests pro Tag, und die Prüflast bleibt menschengerecht, weil die Regeln die Fehlermodi früh abfangen. Ein Team, das die Checkliste übernimmt, behält die Geschwindigkeit und verliert den Wochenend-Incident. Das ist der ganze Tausch - es gibt keine Version, in der die Disziplin optional ist und das Ergebnis gleich bleibt.

Dieses Dokument ist Teil der UHL-Ressourcen. Direkter Download und verwandte Arbeiten:

<https://uhl.cloud/de/resources/>

